IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF Item #1: Vortex Cell Phone, Model # HD62, Serial Number HD6200169318 IMEI: 350733791693189; CURRENTLY LOCATED AT FBI HEADQUARTERS in Salt Lake City, 5425 Amelia Earhart Drive, Salt Lake City, Utah 84116.	Case No. 2:24mj461-DAO

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Justin Hansen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, electronic devices, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachments A and B.

2. Your affiant has been a TFO with the Federal Bureau of Investigation since 2018 and is currently to the FBI Violent Crimes Task Force/Child Exploitation Human Trafficking Task Force. Your affiant has been involved in investigations related to violent crimes, sexual exploitation of children, and sexual abuse of children since 2018.

Your affiant has gained experience through training in seminars, classes, and everyday work related to conducting these types of investigations. Your affiant has been involved in numerous investigations involving violent crimes, violent crimes against children, internet crimes against children, and sex crimes against children, to include leading investigations related to violent crimes, aggravated sexual abuse of children, kidnappings, child pornography, writing and executing search warrants, collecting evidence, interviewing victims, interviewing suspects, and conducting arrests.

3. As a TFO, your affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) and (e) (production of child pornography); 18 U.S.C. § 2252A(a)(5)(B) (possession of and access with intent to view child pornography); are presently located on Subject's devices.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

The property to be searched is as follows and is currently located at FBI Headquarters in Salt Lake City, 5425 Amelia Earhart Drive, Salt Lake City, Utah 84116:

Item #1: Vortex Cell Phone, Model # HD62, Serial Number HD6200169318
IMEI: 350733791693189

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachments A and B.

STATUTORY AUTHORITY

6. As noted above, this investigation concerns alleged violations of the following:

7. 18 U.S.C. § 2251(a) and (e) prohibit any person from knowingly employing, using, persuading, inducing, enticing or coercing any minor to engage in, or having a minor assist any other person to engage in, or transporting a minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct.

8. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of

interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

PROBABLE CAUSE

9. On May 6,2023, an unknown male entered the Fred Meyer Jewelers inside the Smith's Marketplace in Bountiful located at 555 South 200 West. The male was described as wearing a black parka with fur around the hood, white sweatshirt, and camouflage mask. The male was carrying a hatchet in his right hand and a handgun in his left. The male began to smash the top of a glass display case with the hatchet. As the male continued to strike the glass a Fred Meyer Jeweler employee confronted the suspect. The suspect turned around, facing the employee and pointed the handgun in his direction. The employee immediately began to back away fearing for his safety and went into a back room to warn another employee. The suspect began reaching in the display case, grabbing jewelry, and putting it in a bag. The male suspect then ran out of the store, leaving the hatchet on the display case. The aggravated robbery was caught on the in-store surveillance video.

10. Local police agencies responded to the area to search for the suspect. During a K-9 search a camouflage balaclava was located at approximately 850 South 200 West in Bountiful. From Smiths Marketplace video surveillance the balaclava the suspect was wearing during the robbery is the same found by officers. The hatchet and

balaclava were taken into custody by Bountiful Police Department officers and submitted to the Utah State Crime Lab for testing. On January 5, 2024, Bountiful Police received results from the testing. State Crime lab reported they located four DNA profiles on the hatchet and did not test further. However, on the balaclava an unknown male #1 was obtained and would be run through national and local database. On January 17, 2024, Bountiful Police Department received a follow up result letter. The letter stated the unknown male #1 DNA had hit in CODIS and Matched Carlos Anthony Martinez.

11. In the interim following the robbery that occurred on May 6, 2023, on November 30, 2023, UHP Troopers responded to an attempt to locate/ automobile crash on SR-67 (Legacy Highway). The driver was identified as Carlos Anthony Martinez. Two juvenile females were found to be in the vehicle with Martinez. One identified as a 15-year-old female, the other a 14-year-old female. After failing field sobriety tests, UHP Troopers attempted to take Martinez into custody for DUI. Martinez began to pull away in an attempt to escape. A struggle ensued where an additional trooper had to assist in taking him into custody. After getting Martinez into hand cuffs a Springfield Hellcat handgun with a bullet in the chamber and a full magazine were located in the front right pocket of Martinez pants. Martinez was booked on felony and DUI charges. A follow up investigation was done by the Utah State Bureau of Investigation regarding the juvenile females in the vehicle. The females were intoxicated and suspected to have used alcohol and narcotics supplied by Martinez. The 15-year-old female (Victim #1) stated she was Martinez's girlfriend. The 14-year-old (Victim #2) stated she was a friend of Victim #1 and she and Martinez had picked her up. Both Victims were released to

parents. Later in the day Victim #2 called Salt Lake City Police Department to report she had been drugged the night before and sexually assaulted by Martinez.

12. While conducting the investigation an SBI Agent requested and was granted a search warrant for Martinez' phone. After receiving the "download" of Martinez' phone, the investigator discovered two pictures of Martinez and Victim #1 laying by each other cheek to cheek in a "spooning" position. The image showed Martinez taking a picture while Victim #1 was topless showing her naked breasts. A video of the same position showed Martinez rubbing her naked breast with his hand. The video is only a few seconds long. A still shot of the video shows her breasts covered by an image which appears to be from Snapchat. Several additional nude topless pictures of Victim #1 were located on the download.

13. Martinez continues to attempt to contact Victim #1, by texting Victim #1's relatives. Martinez has also told relatives of Victim #1 he believes he gave her an STD. Martinez has been advised Victim #1 is a juvenile and to not contact Victim #1. Martinez has also sent what he claimed to be an "UBER" driver to Victim #1's residence to pick her up. A witness observed the "UBER" at the residence and observed two unknown juvenile females in the back seat that appeared to be intoxicated. The initial investigation determined it was not an UBER driver, however possibly a relative or associate of Martinez.

14. During the investigation your affiant gained firsthand knowledge that Martinez used and continued to use an electronic devices to communicate with, receive,

and capture images of nude juvenile females. Currently, it is unknown exactly which devices Martinez utilized.

15. Several electronic devices were discovered during the execution of a search warrant of the defendant's home, located at 1958 W Black Angus Drive, Salt Lake City, Utah on April 12, 2024, including the above described Vortex cell phone which was found in his bedroom on the defendant's nightstand charging next to his bed. However, when initially seized the Vortex cell phone it was believed to be an iPhone. The Devices are currently in the lawful possession of the FBI. Therefore, while the FBI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

16. Federal search warrants were obtained for all devices including the misidentified Vortex cell phone. Chief Magistrate Judge Dustin Pead signed the search warrants on April 29, 2024, case no. 2:24mj00442 DBP.

17. On May 6, 2024, the misidentified Vortex cell phone was to be analyzed, but when technicians went to examine the cell phone and removed the cover, they identified the cell phone as a Vortex cell phone not an iPhone as previously believed. The examination did not proceed and is awaiting a revised search warrant.

18. The Device is currently in storage at the FBI Headquarters evidence room in Salt Lake City, Utah. In my training and experience, I know that the Devices have

been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may

also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash

memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address

is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

k. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not

necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

l. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

m. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central

processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

n. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

o. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

p. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

q. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

r. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

s. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

t. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

u. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions,

including engaging in online chat and sending or receiving images and videos.

v. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

w. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

x. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

20. Based on my training and experience I know that suspects who have committed aggravated robberies and possession of child pornography typically have evidence pertaining to those robberies in their residence or on personal electronic devices. This evidence typically includes clothing worn during the commission of the robbery; weapons or ammunition; and or other evidence taken during the commission of the robbery. Additionally, electronics including cellular phones; tablets; or other devices used to communicate with minor's or capture images and are used for the production and possession of child pornography. Based on my training, and experience, I know that the

Devices have capabilities that allow it to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file. Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs

store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine the devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device as described in Attachment A to seek the items described in Attachment B.

Dated this 6th day of May 2024.

Respectfully submitted,

Justin Hansen Digitally signed by Justin Hansen
Date: 2024.05.06 17:48:17 -06'00'

JUSTIN HANSEN
Utah State Bureau of Investigations
FBI Task Force Officer

Subscribed and sworn to before me this 7th day of May 2024

BY THE COURT:

Daphne A. Oberg

DAPHNE A. OBERG
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The following items was seized during the execution of a search warrant of the defendants home, located at 1958 W Black Angus Drive, Salt Lake City, Utah on April 12, 2024. The seized item is currently stored in evidence at the FBI in Salt Lake City, 5425 Amelia Earhart Drive, Salt Lake City, Utah 84116:

Item #1: Vortex Cell Phone, Model # HD62,

Serial Number HD6200169318

IMEI: 350733791693189

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. Your Affiant requests to search and seize any digital evidence stored on the listed cellphone or evidence located within any application downloaded on them. This evidence is to include, but not limited to call logs, SMS messages, MMS messages, chats, photos, videos, geo locations logged on the phone, contact lists, emails, and any other digital evidence found to be in relation to crimes listed in this affidavit. Your Affiant requests to complete both electronic and manual searches of the devices.

2. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 2251(a) and (e) (production of child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography and involve Carlos Anthony Martinez since on or before May 6, 2023, including:

a. call logs, SMS messages, MMS messages, chats, photos, videos, geo locations logged on the phone, contact lists, emails, and any other digital evidence found to be in relation to crimes listed in this affidavit;

b. any information recording Carlos A. Martinez's schedule or travel out of the state of Utah to the present;

c. depictions of minors engaged in sexual activity.

3. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

4. Records evidencing the use of the Internet Protocol addresses to communicate with minor female victims, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.